HORIZON3.ai

How HORIZON3.ai Strengthens Supply Chain Security for CMMC

Whitepaper

Summary

HORIZON3.ai provides the real-time, robust, evidence-based approach to mitigating supply chain risk by supporting DOW contractors and their suppliers in meeting CMMC requirements.

A perfect example of this type of approach was when the target was a production environment supporting globally significant operations exactly the type of supplier an adversary would prioritize as geopolitical tensions rise. With no human operators involved, no prior knowledge of the environment, and without disrupting critical production systems, NodeZero achieved full domain compromise in under six hours.

The engagement was executed as an assume-breach test: NodeZero began with access to a single host, no credentials, and basic network reach, akin to obtaining a shell on one machine. From there, it enumerated local domain users and successfully executed a password spray to obtain a valid domain user credential. That account unexpectedly had local administrator rights, allowing NodeZero to deploy a remote access tool (RAT) running as SYSTEM, dump LSASS, and harvest additional user credentials—evidence that endpoint detection and response controls were either missing or misconfigured on that host.

NodeZero then abused an Active Directory ACL misconfiguration to elevate privileges, exfiltrate a PFX certificate (a user's private key), and use it to access DPAPI secrets, yielding still more credentials. With this growing credential set, NodeZero conducted further password spraying and exploited a vulnerable ADCS template, ultimately escalating to Domain Admin and taking full control of the environment. In total, the attack path chained eight weaknesses across six hosts, leveraging seven compromised credentials buried within a large, complex network.

Notably, no CVEs or traditional software exploits were required; the compromise relied entirely on weak Active Directory configurations, poor credential hygiene, and ineffective EDR configurations. The report highlights that remediating five Systemic weaknesses (which are identified and described in Node Zero Pentesting reports) across the estate would dramatically reduce risk. Finally, the tactics used to achieve Domain Admin mirror known Iranian threat actor tradecraft, underscoring that defending against real-world adversaries demands more than Checklists and marketing hype: it requires AI pentesting that continuously stress-tests organizations against live, nation-state-level TTPs.

NodeZero Attack Path Described Above

CMMC Program Levels

The updated CMMC Program outlines three maturity levels, each integrating security standards from existing regulations and guidelines:

Level 1: Basic Safeguarding of Federal Contract Information (FCI)

Requirements:

+ Compliance involves an annual self-assessment and affirmation of the 15 security requirements specified in FAR clause 52.204-21.

Level 2: Broad Protection of Controlled Unclassified Information (CUI)

Requirements:

+ Compliance must be verified with an annual affirmation for the 110 security requirements in NIST SP 800-171 Revision 2.
+ A triennial assessment is also required, which may be a self-assessment or an independent assessment by an authorized CMMC Third-Party Assessment Organization (C3PAO). The type of assessment is determined by the contract, specifically based on the information (processed, transmitted, or stored CUI) on the contractor or subcontractor information systems.

Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats (APTs)

Requirements:

- Requires first achieving Final Level 2 CMMC Status.
- A triennial assessment is conducted by the Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
- An annual affirmation is necessary to verify compliance with the 24 identified requirements from NIST SP 800-172.

NodeZero Proactive Security Practices

DIBs exploring CMMC at a high level will notice that HORIZON3.ai NodeZero offers the following proactive security practices that show real impact to their mission and compliance to the Goals of CMMC.

Continuous Security Validation with NodeZero NodeZero delivers continuous, autonomous security validation that goes beyond traditional annual assessments.

- **Comprehensive Coverage:** It executes autonomous penetration tests across your and your suppliers' internal, external, cloud, on-premise, and hybrid environments.
- **Risk-Prioritized Insights:** Findings are prioritized based on actual impact and exploitability, providing a more meaningful assessment than a simple vulnerability count.
- **Compliance-Ready Evidence:** The platform automatically generates the evidence necessary to populate your System Security Plan (SSP), Plan of Action & Milestones (POA&M), and other essential CMMC documentation.

Extending Trust-But-Verify assurance to suppliers. HORIZON3.ai enables prime contractors to move past relying solely on vendor attestations and questionnaires by establishing an evidence-based "trust but verify" security model across the supply chain.

- **Post-Remediation Confirmation:** Use NodeZero to validate the security posture of critical suppliers handling Controlled Unclassified Information (CUI) or key mission systems.
- **Effective Remediation Confirmation:** Verify that remediation efforts were truly effective, rather than merely accepting a vendor's word.

+ **Standardized Evaluation:** Implement repeatable, standardized security evaluations across multiple suppliers for consistent risk management.

Mapping Outcomes Directly to CMMC Requirements. NodeZero's outputs are designed to align directly with CMMC expectations

+ **Risk Management:** Findings and verified exploit paths feed directly into your risk register and Risk Management (RM) practices.
+ **System Security Plan (SSP) Maintenance:** Validated controls provide data for SSP updates and ongoing continuous monitoring records.
+ **Demonstrating Risk Reduction:** Retesting after implementing fixes provides updated POA&M documentation, clearly demonstrating risk reduction over time.

This integrated approach ensures that both prime contractors and their suppliers can provide concrete evidence of continuous due diligence, rather than just a one-time compliance snapshot.

How to Use This Mapping

DIBs exploring CMMC at a high level will notice that HORIZON3.ai NodeZero offers the following proactive security practices that show real impact to their mission and compliance to the Goals of CMMC.

CMMC Level 2 / NIST SP 800-171

Use Section 1's per-control mapping in SSP/POA&M language. Specify NodeZero provides technical verification/evidence; policy/process ownership remains with the organization.

Go to Mapping →

CMMC Level 3 / NIST SP 800-172

Pair Section 2's family-level mappings with the 24 enhanced requirements (CFR Table 1). This area describe HORIZON3.ai NodeZero as the adversary-emulation and continuous-validation engine supplying the technical proof for these enhanced controls.

Go to Mapping →

NodeZero Mapping to NIST SP 800-171 & 800-172 (CMMC)

This mapping focuses on the NIST SP 800-171 Rev. 2 controls and related CMMC Level2 practices that NodeZero can technically verify or inform, plus a higher-level mapping for the NIST SP 800-172 enhanced requirements used at CMMC Level3

NIST SP 800-171 Rev. 2 Controls NodeZero Directly Supported

The table below aligns CMMC Level 2 practices to their underlying NIST SP 800-171 controls, and summarizes how NodeZero is used and what functionality it exercises.

1.1 Risk Assessment (RA) & Security Assessment (CA)

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.11.1	RA.L2-3.11.1 – Risk Assessments	Periodic risk assessment of systems processing CUI	Continuously measures and reports on overall exploitable attack surface (trends in attack paths, weaknesses, impacts) to feed the risk register and risk analysis for CUI systems.	Autonomous internal/ external pentests, attack-path analytics, risk trending (MTTR/MTTM when used with Insights).
3.11.2	RA.L2-3.11.2 – Vulnerability Scan	Vulnerability scanning on CUI systems and apps	Runs autonomous network pentests that go beyond CVE checklists, continuously identifying exploitable weaknesses; Rapid Response tests new N-day threats proven to affect the environment; satisfies “periodic” and “when new vulnerabilities are identified” expectations by running on a defined cadence and in response to new KEVs.	Autonomous pentesting, Rapid Response KEV/N-day exploit checks, continuous scheduling (“Pentest Wednesday®”).

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.11.3	RA.L2-3.11.3 – Vulnerability Remediation	Risk-based remediation of vulnerabilities	Prioritizes exploitable weaknesses by real impact and exploitability, provides concrete remediation guidance, and uses 1-Click Verify to retest after fixes so you can demonstrate that vulnerabilities were actually remediated per risk assessment.	Exploit-based prioritization, remediation guidance, 1-Click Verify retesting, trend metrics (recurrence rate, MTTR).
3.12.1	CA.L2-3.12.1 – Security Control Assessment	Assess if controls are implemented and effective	Emulates real attackers to continuously exercise technical controls (network, identity, EDR/SIEM, segmentation, data access) and shows where they fail in real attack chains; includes specific EDR/SIEM effectiveness tests.	Autonomous adversary emulation across internal, external, AD, segmentation; EDR Effectiveness and SIEM/IDS validation.
3.12.2	CA.L2-3.12.2 – Plan of Action (POA&M)	Plans to correct deficiencies/ vulnerabilities	Supplies proof-based findings that drive POA&M entries (deficiencies, exploit paths, business impacts) and prioritizes them; then re-tests to supply evidence that POA&M items were closed and risk reduced.	Pentest reports structured for POA&M input, remediation sequencing, and verification runs for closure evidence.
3.12.3	CA.L2-3.12.3 – Security Control Monitoring	Ongoing monitoring of control effectiveness	Uses scheduled pentests via NodeZero Runner and on-demand tests after changes/patches to provide continuous assurance that key controls remain effective over time.	Runner-based scheduling, recurring internal/external/ segmentation tests, continuous validation loop (Hack-Fix-Verify-Repeat).

1.2 Access Control (AC) & Identification and Authentication (IA)

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.1.5	AC.L2-3.1.5 – Least Privilege	Limit privileges to what's needed	Attempts privilege escalation and lateral movement using discovered or injected credentials to show where least-privilege boundaries fail (e.g., users with unnecessary local admin/domain rights).	Credential harvesting & reuse, AD attack-path chaining, lateral-movement modules, RAT-based post-exploitation.
3.1.7	AC.L2-3.1.7 – Privileged Functions	Control privileged operations	Targets privileged functions by stealing or abusing elevated accounts (credential dumping, token theft, RAT deployment) to prove where privileged operations can be misused and whether monitoring/ controls catch it.	Privileged-account compromise, RAT deployment, EDR/SIEM visibility checks on privileged activity.
3.1.20	AC.L2-3.1.20 – External Connections (CUI)	Verify/limit external connections handling CUI	Performs external pentests against public-facing services to validate ingress/egress controls, firewall rules, and exposure of CUI-relevant services, showing which external connections can be abused in practice.	External pentesting, internet-exposed service enumeration, exploit chains from internet to internal/CUI assets.
3.1.22	AC.L2-3.1.22 – Control Public Information (CUI)	Control CUI-relevant data on public systems	Uses OSINT modules to discover domains, weak password terms, developer repos, etc., that an attacker can leverage; informs controls to keep CUI and CUI-enabling information off public systems or tighten exposure.	OSINT discovery (domains, Git, credentials), internet footprint analysis feeding AC/communications policies.

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.5.2	IA.L2-3.5.2 – Authentication (CUI)	Proper authentication before access	Attempts logons to services (AD, web, VPN, databases, SaaS) with discovered/injected credentials to validate that authentication is enforced correctly and that weak/breached credentials are not silently accepted.	Credential-stuffing & spraying, service-specific auth checks (Kerberos/NTLM, HTTP, RDP, SSH, VPN, DB).
3.5.7	IA.L2-3.5.7 – Password Complexity	Strong password policy/enforcement	Runs the Active Directory Password Audit to find weak, breached, and reused passwords and to test "weak password terms" (from OSINT or org-provided lists) across the AD population, evidencing whether complexity and change-of-character rules are working.	AD Password Audit, dictionary/rainbow-table checking, breached-password detection, OSINT-derived weak terms testing.
3.5.10	IA.L2-3.5.10 – Cryptographically Protected Passwords	Protect passwords at rest/in transit	During AD Password Audits and internal tests, NodeZero discovers cleartext and hashed credentials, extracts them from LSASS/AD and validates whether they are stored and handled using cryptographically secure mechanisms as required by the control.	Credential-dumping modules (LSASS, DPAPI), AD Password Audit, analysis of hash types and storage locations.

1.3 System and Information Integrity (SI)

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.14.1	SI.L2-3.14.1 – Flaw Remediation	Identify, report, and correct system flaws	Identifies exploitable flaws (vulns + misconfigurations) across internal/ external scopes on a customer-defined cadence, provides detailed remediation guidance, and allows retesting to prove corrections occurred within required timeframes.	Autonomous pentests, vuln & misconfig discovery, remediation guidance, retest campaigns, MTTR/ recurrence metrics.
3.14.2	SI.L2-3.14.2 – Malicious Code Protection	EDR/AV effectiveness	Attempts to deploy and operate its internal Rust-based RAT and other post-exploitation actions to validate whether EDR/AV and endpoint protections detect or block malicious-code-like behaviors in production, informing tuning of those tools.	Endpoint Security Effectiveness tests, RAT deployment, telemetry correlation with EDR/SIEM.
3.14.3	SI.L2-3.14.3 – Security Alerts & Advisories	Act on new threat advisories	The Rapid Response capability monitors emerging N-day/zero-day advisories and delivers exploit checks directly in NodeZero; organizations run targeted tests to see if newly disclosed threats are exploitable in their environment, then prioritize remediation accordingly.	Rapid Response KEV/N-day modules, targeted exploit checks, advisory-driven test templates.
3.14.5	SI.L2-3.14.5 – System & File Scanning	Periodic & real-time scanning	Uses exploitation plus Sensitive Data Exposure / ADP features to inspect files and data stores it reaches (pattern-matching & NLP for PII/ PHI/CUI) and to surface where data is exposed because of weaknesses, complementing traditional malware/file scanning.	Data-pilfering modules, Advanced Data Pilfering (ADP), sensitive-data classifiers, file share exploration.

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.14.6	SI.L2-3.14.6 – Monitor Communications for Attacks	Monitor inbound/ outbound traffic	Simulated attacks—including MITM with Cyanide, lateral movement, and C2-like traffic—test whether IDS/IPS/SIEM and network monitoring detect malicious communications in both directions, and where gaps exist.	MITM/Cyanide modules, C2 simulations, correlation against SIEM/IDS alerts.
3.14.7	SI.L2-3.14.7 – Identify Unauthorized Use	Find unauthorized system use	Chains weaknesses and compromised credentials to simulate unauthorized use of systems (e.g., illegitimate logons, privilege abuse, unexpected data access), giving concrete examples that should be flagged by behavioral analytics, UEBA, or SOC processes.	Credential abuse, lateral movement, unusual logon/ activity patterns visible to SIEM/EDR/UEBA tooling.

1.4 Configuration Management (CM) & System and Communications Protection (SC)

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.4.2	CM.L2-3.4.2 – Security Configuration Enforcement	Enforce secure configuration baselines	Detects exploitable misconfigurations in OS, network, cloud, and identity configurations (e.g., weak crypto, insecure defaults, missing hardening) and links them to real attack paths, evidencing whether defined secure configuration baselines are truly enforced.	Misconfiguration discovery across infra/AD/cloud, attack-path validation, mapping findings to config standards (NIST/ benchmarks).

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.4.6 / 3.4.7	CM.L2-3.4.6 / 3.4.7 – Least / Nonessential Functionality	Only essential services, ports, protocols	Uses segmentation testing and internal pentests to enumerate reachable services, ports, protocols, and applications, then highlight unnecessary exposures (e.g., legacy protocols, admin interfaces) that violate least-functionality principles.	Segmentation tests, port/service enumeration, exploit-based validation of "unnecessary" services.
3.4.8	CM.L2-3.4.8 – Application Execution Policy	Whitelisting/ blacklisting enforcement	Attempts to execute its RAT and other payloads on compromised hosts, validating whether application control (whitelisting/blacklisting, EDR policies) actually prevent unauthorized code execution as defined in the organization's policy.	RAT execution attempts, application-control bypass tests, EDR policy validation.
3.13.1	SC.L2-3.13.1 – Boundary Protection (CUI)	Monitor/control/ protect comms at boundaries	Internal, external, and segmentation tests validate boundary protections (firewalls, gateways, VLAN boundaries) by demonstrating which traffic and attack paths actually traverse external and key internal boundaries to CUI systems.	External/internal pentests, segmentation assessments, cross-boundary lateral movement, Zero-Trust boundary validation.
3.13.4	SC.L2-3.13.4 – Shared Resource Control	Prevent unintended info transfer via shared resources	Exploits shared resources such as file shares, misconfigured permissions, and shared credentials to locate and exfiltrate sensitive data (PII/PHI/CUI), testing the effectiveness of shared-resource and data-access controls.	File-share abuse, permission abuse, Sensitive Data Exposure / ADP scanners.
3.13.6	SC.L2-3.13.6 – Deny by Default / Permit by Exception	"Deny all, permit by exception" network policy	Probes network paths and services to see which ports/protocols are actually reachable, validating that deny-by-default and allow-by-exception rules are correctly implemented on firewalls and other enforcement points.	Network enumeration from multiple vantage points, firewall rule/ACL testing via real exploitation attempts.

1.5 Audit and Accountability (AU) & Incident Response (IR)

NIST 800-171 Control	CMMC L2 Practice	Control Theme	How NodeZero Can Be Used	NodeZero Functionality Type
3.3.1 / 3.3.2	AU.L2-3.3.1 / 3.3.2 – Audit Logs & User Accountability	Create/retain logs; trace actions to users	Generates high-fidelity attack activity (including Insider-style attacks with injected credentials) that should be logged and correlated back to specific users, helping validate that audit policies, log content, and SIEM pipelines can uniquely trace user actions.	Attack campaigns as logging test cases, insider-style operations, SIEM/UEBA correlation checks.
3.6.1	IR.L2-3.6.1 – Incident Handling	Full IR lifecycle capability	Tripwires plant honey-credentials/ tokens on real attack paths discovered during pentests; when a real adversary touches them, they immediately alert SOC/IR, serving as high-signal triggers that exercise detection, analysis, containment, and recovery steps.	NodeZero Tripwires™, high-fidelity decoys, integration with SIEM/ SOAR/SOC runbooks.
3.6.3	IR.L2-3.6.3 – Incident Response Testing	Test IR plan and capability	Internal pentests, Rapid Response tests, and targeted scenarios act as realistic incident-simulation events, allowing teams to validate their IR plans, communications, and tooling against objective attack activity.	Planned & ad-hoc campaigns used as purple-team / IR exercises, evidence into IR post-mortems and improvement cycles.

NIST SP 800-172 Enhanced Requirements (CMMC Level 3)

2.1 Scope and Relationship to NodeZero

Per CMMC guidance and the 32 CFR 170 rule, CMMC Level 3 adds 24 enhanced requirements from NIST SP 800-172 on top of the 110 NIST SP 800-171 controls, targeting resilience against Advanced Persistent Threats (APTs).

HORIZON3.ai NodeZero Federal is already used to produce evidence for NIST 800-171/172 control effectiveness, particularly across the RA, AC, IA, AU, IR, SI, and SC families, and that these mappings are used in FISMA, FedRAMP, CMMC 2.0, and Zero Trust programs. The detailed list of the 24 specific enhanced requirements comes from Table 1 in 32 CFR § 170.14(c)(4), which is not text-indexed here; the table below therefore maps NodeZero to the main NIST SP 800-172 capability areas rather than reproducing each enhanced control verbatim.

2.2 High-Level Mapping: 800-172 Enhanced Themes to NodeZero Capabilities

800-172 Enhanced Focus Area (Family)	Example CMMC L3 Practice / Theme	How NodeZero Supports the Enhanced Requirement Set	NodeZero Functionality Type
Risk Assessment (RA) – APT-aware risk mgmt	Enhanced, threat-informed risk assessment over time	Continuous autonomous pentests (internal, external, cloud, AD, segmentation) generate attack-path-validated risk data tied to APT-like TTPs (mapped to MITRE ATT&CK), supporting enhanced RA expectations for realistic, threat-driven analysis rather than static scoring.	Autonomous adversary emulation, ATT&CK-mapped findings, risk trending (MTTR/ MTTM, recurrence).
Security Assessment (CA) – Advanced control effectiveness	Annual/ongoing penetration testing and advanced verification (e.g., CA.L3-3.12.1e)	NodeZero serves as the technical engine for Level 3 penetration-testing requirements, supplying repeatable, evidence-rich tests that show whether enhanced controls (segmentation, identity hardening, EDR, Zero-Trust policies) stand up to APT-style attack paths.	FedRAMP High NodeZero Federal™, internal/external/ cloud/segmentation tests, 1-Click Verify, Zero-Trust control cross-walks.

800-172 Enhanced Focus Area (Family)	Example CMMC L3 Practice / Theme	How NodeZero Supports the Enhanced Requirement Set	NodeZero Functionality Type
Access Control (AC) & Identification/ Authentication (IA) – APT-resilient identity	Stronger protection of privileged access, credentials, and identity systems under APT pressure	NodeZero relentlessly attacks identity fabric—AD, Entra ID, local accounts, service accounts, MFA roll-out—using password audits, credential theft, pass-the-hash/token abuse, and identity-centric attack paths, evidencing how well enhanced AC/IA measures withstand a determined adversary.	AD/Entra attacks, password audit, credential-spray/stuffing, privileged abuse, lateral movement to crown-jewel data.
Audit & Accountability (AU) – High-fidelity telemetry under attack	Enhanced logging, correlation, and protection of audit data in APT scenarios	Because all NodeZero operations are mapped to TTPs and attack paths, they provide concrete, repeatable cases to confirm that enhanced AU controls (time-sync, cross-system correlation, protection of logs, real-time analytics) detect and retain evidence of sophisticated campaigns.	Controlled attack campaigns as AU test cases, SIEM content validation, audit log protection/ coverage checks.
Incident Response (IR) – Advanced, tested IR	Enhanced, APT-oriented IR planning, rehearsal, and performance measurement	NodeZero-driven campaigns (including Rapid Response-driven tests and dedicated purple-team scenarios) allow organizations to exercise Level 3 IR procedures—from early detection to containment and eradication—against realistic threat activity, producing metrics and evidence for 800-172 IR enhancements.	IR playbook testing, Tripwires™/ decoys, advanced scenarios (insider, supply-chain, identity compromise).
System and Communications Protection (SC) – Hardened Zero-Trust boundaries	Stronger segmentation, encrypted communications, and APT-resistant architectures	Segmentation and Zero-Trust-oriented tests validate that micro-segmentation, SDN, encrypted tunnels, and boundary policies really block cross-segment attack paths, lateral movement, and data exfiltration even when credentials and internal footholds are compromised (a core 800-172 theme).	Segmentation tests, boundary-evasion attempts, encrypted-path validation, Zero-Trust pillar assessment (User, Device, Network, App, Data).

800-172 Enhanced Focus Area (Family)	Example CMMC L3 Practice / Theme	How NodeZero Supports the Enhanced Requirement Set	NodeZero Functionality Type
System and Information Integrity (SI) – APT-resilient detection and hardening	Enhanced flaw remediation, malicious-code defense, behavioral detection	NodeZero's Endpoint Security Effectiveness, Rapid Response, ADP, and Threat Actor Intelligence provide a continuous feed of realistic malicious behaviors—privilege escalation, RAT deployment, C2-like traffic, data theft—that test whether enhanced SI controls detect, contain, and support rapid flaw remediation under APT conditions.	EDR/AV effectiveness tests, KEV/N-day exploit checks, data-pilfering, threat-actor–aligned campaigns.

Important caveat:

+ The exact 24 NIST SP 800-172 requirements referenced in 32 CFR § 170.14(c)(4) are legally authoritative and should come from the CFR/NIST texts themselves. The table above is intentionally framed at the family/theme level to avoid guessing at individual enhanced-control wording while still showing where NodeZero practically contributes evidence for those Level 3 expectations.